

CENTRO UNIVERSITÁRIO ATENAS

LARISSA DUANE NEIVA LIMA

**A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E O
ACOMPANHAMENTO DAS LEIS BRASILEIRAS**

Paracatu-MG

2020

LARISSA DUANE NEIVA LIMA

**A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E O ACOMPANHAMENTO DAS
LEIS BRASILEIRAS**

Monografia apresentada ao curso de Direito do
Centro Universitário Atenas, como requisito
parcial para obtenção do título de Bacharel em
Direito.

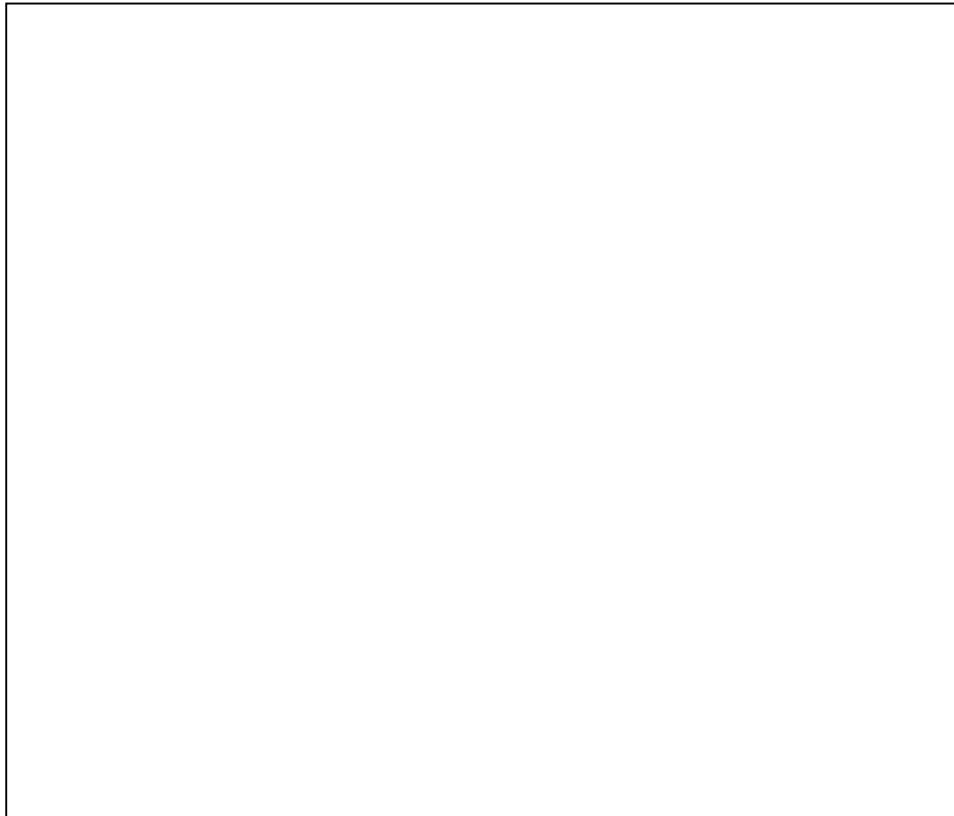
Área de concentração: Ciências Sociais

Orientadora: Prof^ª. Msc. Erika Tuyama

Paracatu - MG

2020

FICHA CATALOGRAFICA

A large, empty rectangular box with a thin black border, occupying the lower half of the page. It is intended for entering cataloging data.

LARISSA DUANE NEIVA LIMA

**A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E O ACOMPANHAMENTO DAS
LEIS BRASILEIRAS**

Monografia apresentada ao curso de Direito do
Centro Universitário Atenas, como requisito
parcial para obtenção do título de Bacharel em
Direito.

Área de concentração: Ciências Sociais

Orientador: Prof^a. Msc. Erika Tuyama

Banca Examinadora:

Paracatu-MG, de de 2020.

Prof^a. Msc. Erika Tuyama
Centro Universitário Atenas

Prof. Msc. Altair Gomes Caixeta
Centro Universitário Atenas

Prof. Msc. Diogo Pereira Rosa
Centro Universitário Atenas

AGRADECIMENTOS

Agradeço primeiramente a Deus que me ajudou na busca de inspiração e determinação para a elaboração deste trabalho e agradeço também aos meus pais, familiares e amigos que de alguma forma me auxiliaram no estudo e elaboração do presente estudo.

"bonis nocet, qui malis parcit"

(ditado em latim)

RESUMO

Presente trabalho é uma análise dos crimes que são cometidos com o uso ou não da internet, por meio de dispositivos eletrônicos, sabendo que, tanto os aparelhos quanto os meios de praticar os delitos se encontram em constante evolução.

A evolução da sociedade é gradual, assim como os problemas enfrentados no decorrer dos dias, da época, da década, do século. No decorrer desta evolução os entendimentos sobre direitos e deveres se ampliam, ou seja, evoluem junto com a sociedade e sua forma de pensar. O direito busca acompanhar essa evolução sempre com intuito de aplicar as leis e os entendimentos jurídicos de forma justa e eficaz ao longo do tempo. A sociedade se evolui em todos os campos, seja em seu modo de agir, pensar, produzir, comercializar ou até mesmo em seu modo de sobrevivência e de cometimento de atos ilícitos. Essa evolução trouxe para área da informática virtual grande expansão, suprimento de necessidades e dependência. Pois, hoje em dia, nos vemos dependentes da plataforma virtual para suprir nossas necessidades de se comunicar e para realização de inúmeras coisas como trabalho, estudos e lazer. No entanto, este campo de evolução pode se tornar também um campo de vulnerabilidades, tanto para as vítimas de crimes que podem ser cometidos neste meio, quanto para facilitar o cometimento de condutas criminosas, quando usado por pessoas mau intencionadas. Desta forma, o presente estudo visa avaliar se as leis brasileiras que vigoram em nossa jurisdição estão aptas a tipificar e punir os crimes cometidos no ciberespaço, sendo que estes se encontram em constante evolução.

Palavras- chave: Sociedade. Evolução. Direito.

ABSTRACT

The present work is an analysis of the crimes that are committed with the use or not of the internet, by means of electronic devices, knowing that both the devices and the means of committing the crimes are constantly evolving.

The evolution of society is gradual, as are the problems faced in the course of days, times, decades, centuries. In the course of this evolution, understandings about rights and duties are broadened, that is, they evolve together with society and its way of thinking. The law seeks to accompany this evolution always with the aim of applying laws and legal understandings in a fair and effective manner over time. Society evolves in all fields, be it in its way of acting, thinking, producing, commercializing or even in its way of surviving and committing illegal acts. This evolution brought to the area of virtual computing a great expansion, supply of needs and dependence. Nowadays, we find ourselves dependent on the virtual platform to supply our needs to communicate and to carry out countless things like work, studies and leisure. However, this field of evolution can also become a field of vulnerabilities, both for the victims of crimes that can be committed in this environment, and to facilitate the commission of criminal conduct, when used by people with bad intentions. Thus, this study aims to assess whether the Brazilian laws in force in our jurisdiction are able to typify and punish crimes committed in cyberspace, and these are constantly evolving.

Keywords: Society. Evolution. Right.

LISTA DE FIGURAS

FIGURA 1- Caminho do sinal da internet	16
FIGURA 2- Como a internet funciona	16

SUMÁRIO

1 INTRODUÇÃO	11
1.1 PROBLEMA	11
1.2 HIPÓTESES	12
1.3 OBJETIVOS	12
1.3.1 OBJETIVO GERAL	12
1.3.2 OBJETIVOS ESPECIFICOS	12
1.4 JUSTIFICATIVA DO ESTUDO	12
1.5 METODOLOGIA DO ESTUDO	13
1.6 ESTRUTURA DO TRABALHO	13
2 FUNCIONAMENTO DO CIBERESPAÇO	15
3 CONDUTAS TIPIFICADAS PELA LEGISLAÇÃO VIGENTE	18
4 LACUNAS DA LEGISLAÇÃO	22
5 PENALIDADES IMPOSTAS	24
6 CONSIDERAÇÕES FINAIS	26
REFERÊNCIAS	28

1 INTRODUÇÃO

A sociedade se mantém em constante evolução e o direito deve ampará-la de modo que os indivíduos possam viver de forma harmoniosa entre si.

O crescimento do mundo virtual tem grande influência na evolução da sociedade e consequentemente na vida das pessoas que a integram, visto que, cada vez mais, estas, buscam fazer suas atividades como trabalho, lazer e estudos, de uma forma mais rápida, eficaz e prazerosa. O que é facilmente possível por meio da internet, no entanto, as pessoas passam cada vez mais tempo atrás da tela de um computador, smartphones, e demais aparelhos que possuem conexão ao ambiente virtual, sendo que, para acessá-lo não é necessário se identificar. Desta forma, conseguem conectar-se à rede e se manter no anonimato.

É evidente que a internet trouxe inúmeras vantagens a sociedade, porém, por ter essa possibilidade de acesso anônimo é que muitos indivíduos se aproveitam deste ambiente para cometerem atos ilícitos, se beneficiando da facilidade que o mundo virtual dispõe, pela vinculação de dados e informações.

Diversas são as modalidades de crimes virtuais, que podem ser cometidos neste meio, estando entre eles os crimes contra a honra, (calúnia, difamação e injúria) incitação e apologia a crimes, pedofilia, extorsão, furto de valores bancários, compartilhamentos de imagens íntimas de terceiros, sequestro e furto de dados e conversas confidenciais, dentre outros.

Acontece que o mundo virtual por sua praticidade e facilidade no acesso, acaba fazendo vítimas fáceis, que não possuem conhecimento dos riscos e não tem noção da abrangência que este espaço cibernético possui.

Diante disso, tentarei aqui identificar a eficácia das leis brasileiras vigentes, afim de punir e inibir a prática dessas condutas delituosas, onde estes indivíduos se aproveitam da dificuldade de identificação da autoria, para cometer os atos ilícitos nesta plataforma virtual.

1.1 PROBLEMA

Qual a eficácia das leis brasileiras a fim de punir e inibir o cometimento dos crimes cibernéticos?

1.2 HIPÓTESES

Desde a criação das normas que visavam proteger os internautas dos crimes praticados na web, até hoje, é fato a evolução do Direito como se constata na alteração do Código Penal, devido a criação da Lei 12.737/2012, mas conhecida como Lei Carolina Dieckmann.

No entanto, importa salientar que, esta lei só se aplica se o equipamento contiver um dispositivo de segurança habilitado, deste modo, só há a tipificação penal se o aparelho no qual está sendo invadido contiver alguma senha, ou software de segurança, fazendo com que a lei contenha uma lacuna, pois o equipamento que não houver este dispositivo, poderá ser invadido sem que seja esta ação considerada crime.

Devemos então, estar atentos as criações das normas para que tenham completa abrangência, sendo mais específicas quanto as condutas que podem ser tipificadas, acarretando assim a devida punição a estes atos e aos demais que se derivam deste.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Verificar a possibilidade da criação de leis competentes para punir e coibir a pratica dos atos ilícitos, consumados na plataforma virtual.

1.3.2 OBJETIVOS ESPECÍFICOS

- a) Verificar a necessidade de criação de normas especificas para adequar a evolução dos crimes cibernéticos às tipificações penais;
- b) Analisar a descrição das tipificações penais existentes que se amoldem as variadas condutas ilícitas cometidas no mundo virtual;
- c) Revisar as penas aplicadas aos crimes cibernéticos, como forma de coibir sua pratica.

1.4 JUSTIFICATIVA DO ESTUDO

Esperando que Direito evolua com a sociedade surge a dúvida de como um Código Penal pode tipificar a conduta ilícita dos crimes virtuais se este é de 1940, surge a necessidade de que a legislação hodierna também evolua, desta forma faz-se necessário a

criação de leis que regulamentassem tais condutas. Contudo, seria adequado dizer que as leis e os códigos brasileiros não conseguem de forma eficaz inibir a prática dos crimes praticados na internet.

Sabemos que os crimes praticados na plataforma virtual podem ser os mais variáveis possíveis, da mesma forma os efeitos que estes atos ilícitos acarretam na vida das vítimas.

Desta forma, surge na sociedade atual um temor de que essa modalidade de crime não seja abarcada pela legislação penal para que coíba a prática de atos ilícitos em um mundo totalmente virtual.

Cabe aos operadores do direito buscar através de normas efetivas a justiça, conseguindo de forma satisfatória punir o sujeito ativo, afim de trazer à vítima satisfação e segurança para ingressar novamente no meio virtual.

O que nos levou a buscar maiores informações com o intuito de contribuir para a coibição de práticas delituosas no ciber mundo, assim esclarecendo a situação atual de nossa legislação para trazer maior segurança jurídica aos usuários da rede mundial de informação.

1.5 METODOLOGIA DO ESTUDO

A pesquisa a ser realizada neste projeto classifica-se como descritiva e explicativa. Isso porque busca proporcionar maior compreensão sobre o tema abordado com o intuito de torná-lo mais explícito.

Quanto à metodologia fez-se a opção pelo método dedutivo. Esta opção se justifica porque o método escolhido permite uma análise aprofundada acerca do tema.

Em relação ao procedimento optou-se por uma abordagem direta.

E por fim, utilizar-se-á de pesquisas bibliográficas, com análises de livros, artigos e outros meios impressos e eletrônicos relacionados ao assunto.

1.6 ESTRUTURA DO TRABALHO

O trabalho foi desenvolvido em cinco capítulos. O primeiro capítulo apresenta o funcionamento do ciberespaço onde são cometidos os delitos cibernéticos.

O segundo capítulo irá analisar as condutas tipificadas pela legislação vigente.

O terceiro capítulo abordará as possíveis lacunas existentes na legislação aplicada aos atos ilícitos cometidos na plataforma virtual.

No quarto capítulo será feito uma análise das penalidades impostas aos delitos virtuais.

Para finalizar no último capítulo são apresentadas as considerações finais do trabalho mostrando se a problemática foi resolvida.

2 FUNCIONAMENTO DO CIBERESPAÇO

A evolução dos crimes praticados nessa plataforma virtual também chamada de ciberespaço é enorme. Primeiramente não podemos falar e avaliar algo do qual não temos ao menos um conhecimento básico, portanto começaremos por entender o que é a internet e o funcionamento do ciberespaço, a qual é o meio empregado para o cometimento dos crimes de que trata este estudo.

Segundo Hugo Cesar Hoeschl (1998), ciberespaço é:

Ambiente gerado eletronicamente, formado pelo homem, as máquinas, a informática e as telecomunicações, onde é possível a prática de atos de vontade, dotado de limites diversos dos tradicionais, norteado e dimensionado fisicamente por comprimentos de onda e frequências, ao invés de pesos e medidas, e não constituído por átomos, mas por correntes energéticas. (p. 15-28)

Segundo o site da Brasil Escola, a internet é:

A Internet é um grande conjunto de redes de computadores interligadas pelo mundo inteiro; de forma integrada viabilizando a conectividade independente do tipo de máquina que seja utilizada, que para manter essa multi-compatibilidade se utiliza de um conjunto de protocolos e serviços em comum, podendo assim, os usuários a ela conectados usufruir de serviços de informação de alcance mundial.

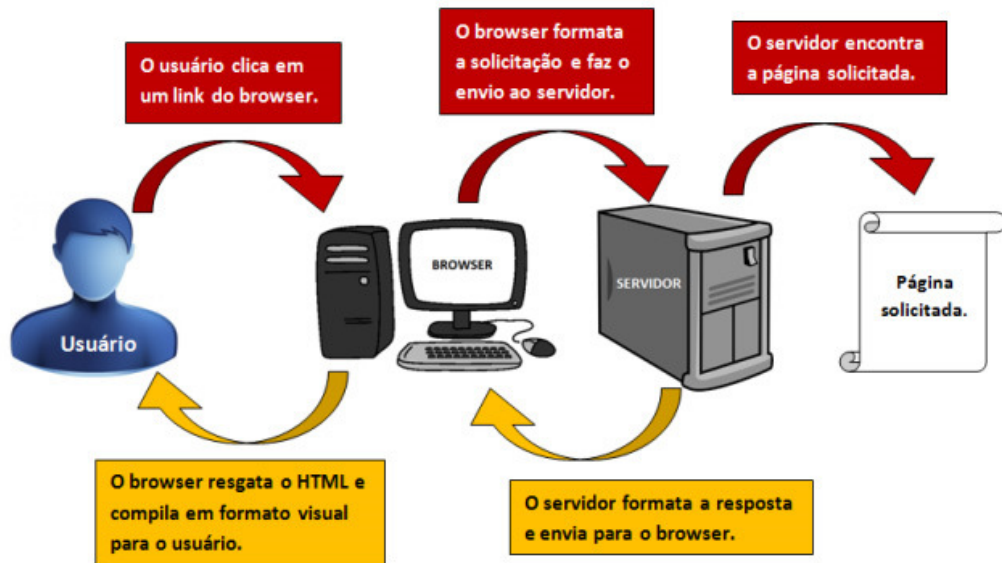
Após estes breves conceitos, passamos a análise dos meios de conexões e funcionalidade. Os tipos de distribuição do sinal de internet, são bem variados, podendo ser por internet móvel, via rádio, fibra óptica, via satélite, via cabo e outros. Bem como os meios de se conectar e usá-la, seja por computador, tvs, smartphones, tablets, smartwhatch, dentre outros.

Explica Raniere Santos, para o site Techtudo (2012):

Este acesso externo ocorre quando a sua rede local se conecta a uma outra rede maior - no caso, o seu provedor de Internet - por meio da tecnologia TCP/IP, um modo de comunicação baseado no endereço de IP (Internet Protocol). Este IP é o endereço de cada um dos pontos de uma rede, e cada ponto da rede consiste em um computador que, por sua vez, se interliga a outros computadores, formando uma verdadeira 'teia de redes'.

Desta forma, podemos analisar as seguintes imagens, para melhores elucidções:

Figura 1



Fonte: **Neto Ferreira**, Caminho até o servidor web.

Diante do que explica Raniere Santos e da imagem analisada acima, podemos constatar basicamente que cada aparelho/dispositivo possui um endereço IP que é único, quando conectado a uma rede local compartilha do mesmo acesso simultâneo que os demais que estiverem nela conectados, ou seja, se conectam à mesma rede de dados e de internet, que por sua vez possui um diferente IP.

Esta rede local, recebe o sinal do seu provedor de internet (que também possui um diferente endereço IP), que é ligado a uma rede maior, que por sua vez é ligada à rede mundial de computadores, formando assim uma teia de acesso, sendo que cada ponto possui um endereço IP único.

Figura 2



Fonte: TECHTUDO, como a internet funciona?

Como podemos ver na imagem acima o caminho da internet se baseia em quatro pontos principais, sendo eles: o Backbone, o provedor de acesso, o provedor de serviço e o usuário final. O primeiro seria o ponto principal de internet e os demais em cadeia vão distribuindo o sinal, sendo que quando o sinal chega ao seu usuário final, pode da mesma forma que receber, o enviar, ou seja, quando se procura por alguma informação o sinal está voltando para o ponto principal para fazer a pesquisa e a resposta volta com o sinal para o usuário final.

Diante da grande quantidade de conexões neste meio cada vez mais as empresas e estabelecimentos fornecem o sinal gratuito à internet, sendo um modo de atrair clientes devido a cada vez mais as pessoas terem o hábito de estarem conectadas à rede.

A sociedade se torna cada vez mais exposta em um ambiente que não oferece segurança aos usuários, pois para usufruir dos seus benefícios não é avaliado critérios como: a sua idade, personalidade, ficha criminal, estado mental, seu passado, presente, etc.

Para melhor entendimento sobre a classificação do crime cibernético, vejamos a descrição de Augusto Eduardo de Souza Rossini (2004 apud DULLIUS, 2012, [n.p.]):

O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Segundo Guilherme Schmidt:

Através do conceito analítico finalista de crime, pode se chegar a conclusão de que crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática. (SCHMIDT, 2014,).

Diante disso, não se pode confiar em quem está do outro lado da rede, pois, é nesse momento em que se fazem as vítimas, e os autores dos crimes não precisam de armas e força física, por exemplo, mas apenas a inteligência e persuasão.

3 CONDUCTAS TIPIFICADAS PELA LEGISLAÇÃO VIGENTE

Um dos objetivos deste estudo é verificar a necessidade de criação de normas específicas para adequar a evolução dos crimes cibernéticos às tipificações penais. Façamos assim, a análise das leis vigentes sobre o tema, existem duas leis que são relacionadas ao cometimento de atos ilícitos por meio da plataforma virtual, a primeira é a Lei dos Crimes Cibernéticos nº 12.737/2012, também conhecida como lei Carolina Dieckmann, por ter envolvido a atriz como vítima de um dos crimes que foi nesta lei prevista.

A outra lei é a 12.965/2014, chamada de Marco Civil, que regula os direitos e deveres dos internautas, visando a proteção e segurança de seus dados e informações, bem como a privacidade e sigilo, onde determina que a quebra de dados e informações particulares só podem se dar por meio de ordem judicial e que as pessoas vítimas dos crimes como o de divulgação de dados e de informações possam requerer a retirada destes do ar.

Importa mencionar também a Lei 12.735/2012 que determina a instalação de delegacias especializadas para combater os crimes virtuais.

Deste modo, em análise a Lei dos Crimes Cibernéticos, citada anteriormente, podemos descrever as tipificações que esta menciona, como:

- Invadir redes, celulares ou algum dispositivo do qual não tenha a autorização, com o intuito de obter informações, instalar algum vírus ou adulterar e fragilizar o dispositivo para prejudicar o proprietário ou quem faz o uso do equipamento;
- Nos cometimentos dos atos acima, o agente na execução, obter conteúdo de comunicação eletrônica que sejam privadas como: e-mails, fotos, senhas, segredos comerciais, controle remoto do dispositivo que foi invadido, etc;
- Após a obtenção dos conteúdos, se o agente vender, transmitir ou divulgar os dados ou as informações que coletou a qualquer pessoa;
- Produzir, oferecer, distribuir, vender ou difundir programa de computador que sirva para cometer os crimes previstos acima;
- Falsificação de cartões de credito ou debito;

É importante analisar a descrição destas tipificações penais existentes que se amoldem aos casos concretos. Pois bem, é cediço que foi grande a evolução da sociedade

desde a criação das normas regulamentadoras de que tratam este estudo, assim como houve crescimento da área informática e virtual, como descreve CRESPO :

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual. (CRESPO, (2011, p.48)

Deste modo, diante de novos conhecimentos é evidente que também fossem expandidos os meios e plataformas para execução dos crimes cometidos no ciberespaço, devendo-se ter cautela quando a análise de cada caso concreto, para a correta aplicação das sanções.

Cada vez mais, há a criação de novas redes sociais, aplicativos, ambientes que disponibilizam e facilitam a comunicação entre pessoas, sabe-se que são amplas as plataformas para cometimentos de tais crimes, sendo disponibilizadas dentro delas várias ferramentas que podem ser usadas de forma a facilitarem condutas delitivas.

Sendo assim, muitas pessoas se vem fragilizadas e prejudicadas diante do seu compartilhamento de dados, que muitas vezes é feita de forma inocente, quando a vítima acaba se envolvendo com seu “agressor”, seja por um relacionamento profissional, emocional, ou até mesmo por um momento de carência ou inocência em questão de idade, pois como dito anteriormente na plataforma se encontram pessoas de todas as idades e intenções. Ocorre que, quando estas pessoas se tornam vítimas destes tipos de crimes, muitas vezes não conseguem prová-los, pois, existem mecanismos para “apagar” informações ou ações das condutas delitivas, além das demais dificuldades enfrentadas pela vítima, assim como na opinião do advogado Daniel Burg em entrevista a Tadeu Rover, para a revista jurídica CONJUR (2017):

A internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão da fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes. “A fronteira acaba motivando também, de certa forma, a impunidade. E aqui, infelizmente, não tem muito o que fazer. Porque não tem como criar uma lei obrigando o cidadão da Estônia a vir para o Brasil no prazo”

Para melhor entendimento, importa a diferenciação dos tipos de sujeitos ativos deste crime. Em uma breve análise, podemos diferencia-los sabendo que possuem diversos graus de periculosidade, como por exemplo, o sujeito ativo pode ser uma pessoa com pouco conhecimento na área, que apenas divulga alguma foto, vídeo, ou informações, etc, de alguma pessoa sem o seu

consentimento. Até uma pessoa com alto grau de conhecimento informático na rede que seja necessário para o cometimento de tal crime. Diante dos diversos tipos de hackers, os que importam para este estudo são os Hackers e os Crackers.

Primeiramente Hack vem do inglês e significa cortar/golpear, por este motivo este termo foi adotado para designar aquelas pessoas que quebram a segurança de outras, o hacker é aquela pessoa que possui interesse e um bom conhecimento na área da informática. Por outro lado, o Cracker foi um termo criado pelos próprios hackers, para que não fossem confundidos, pois o cracker além de ter vasto conhecimento em informática e no funcionamento da rede, a usa de forma maléfica, sendo este o principal sujeitos ativo deste estudo.

Conforme diz Renato Santino para o site Olhar Digital (2013):

As denominações foram criadas para que leigos e, especialmente a mídia, não confundissem os dois grupos. O termo "cracker" nasceu em 1985, e foram os próprios hackers que disseminaram o nome em sua própria defesa. A ideia era que eles não fossem mais confundidos com pessoas que praticavam o roubo ou vandalismo na internet.

Deste modo, o ordenamento jurídico prevendo este tipo de ação, tratou de assegurar os usuários da plataforma quanto ao sigilo de seus dados, como no artigo 7º da Lei 12.965/14, que diz:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (...)

No entanto, essa inviolabilidade poderá ser quebrada por ordem judicial, como se pode ver no inciso II supracitado. Neste caso a regra é que o provedor de internet deve manter os registros de conexões guardados no prazo de 1 (um) ano, porém, há uma exceção por requerimento cautelar da autoridade policial, administrativa ou pelo Ministério Público, citados nos artigos da mesma Lei, abaixo:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

Ainda na mesma Lei é possível perceber que o ordenamento jurídico na tentativa de encontrar o sujeito ativo de delitos cometidos na rede, possibilita a verificação de dados pessoais como endereço residencial dos usuários, conforme o artigo 10º, vejamos:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Sendo que este artigo também prevê a limitação quanto as informações que podem ser prestadas, respeitando os limites da vida privada de cada usuário da rede. Podemos perceber assim, a tentativa de Estado em conseguir identificar os usuários da rede mesmo sem ferir o seu direito à privacidade, sendo feito apenas, em casos excepcionais quando necessário.

4 - LACUNAS DA LEGISLAÇÃO

Percebe-se que as condutas tipificadas no capítulo anterior são basicamente as de invadir ou violar um dispositivo e dele se beneficiar, seja em benefício próprio ou para terceiros, ou fragilizar o sistema, adulterar dados, divulgando informações para prejuízo do proprietário, etc.

O Novo Dicionário de Língua Portuguesa, escrito por Candido de Figueiredo (1913) nos dá a definição de algumas dessas condutas, como as principais:

Invadir: Entrar em. Entrar á força em: *os franceses invadiram Portugal*. Ocupar violentamente. Conquistar. Difundir-se em: *a peste invadiu a Rússia*. (p. 1122)

Violar: ofender violentamente. Transgredir: *violar as leis*. Forçar. Poluir. Atentar contra o pudor de. Profanar. Devassar ou divulgar abusivamente: *violar segredos*. (p. 2091)

Pois bem, este tipo de crime é caracterizado como crime formal, sendo necessário apenas que o agente efetive o mero ato de invadir ou violar o dispositivo para que seja enquadrado na tipificação penal do artigo, não sendo necessário que ele consiga com tal ato, um resultado, como o de vasculhar, coletar dados, etc.

No entanto, diante dessas descrições de condutas, a lei deixou uma lacuna sobre quem invade ou viola dispositivos que não possuem barreiras como por exemplo senhas de acesso e antivírus, e são vasculhados por terceiros, se usados sem autorização do seu proprietário, não merecem tal abrangência pela lei diante de sua conduta de ferir a privacidade do outro?

Desta forma, essa lacuna se dá pelo princípio da legalidade penal, pois não se pode punir condutas que não são previstas em lei, em conformidade com o artigo 5º, XXXIX, da Constituição Federal de 1988: “*não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*”.

Rogério GRECO (2017) diz:

Muito se tem discutido, atualmente, a respeito dos chamados delitos de informática, também reconhecidos doutrinariamente por meio das expressões: crimes de computador, crimes digitais, crimes cibernéticos, crimes via internet, dentre outras.

Segundo NUCCI (2008):

“A norma penal incriminadora, impositiva de sanção, deve ser a última ratio, ou seja, a última hipótese que o Estado utiliza para punir o infrator da lei.”

Deste modo, entende-se que o Direito Penal não vê tipicidade em tais condutas, sendo que sua aplicação só se faz em última ratio. No entanto, a Constituição Federal em seu artigo 5º assegura a inviolabilidade da privacidade, vejamos:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a 17 inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Assegurando assim, indenização as vítimas dos crimes que violem tais direitos, pois, apesar de a legislação específica não abarcar as condutas supracitadas, que ferem a privacidade alheia por meio de dispositivos eletrônicos, a Constituição Federal, trata de assegurar as vítimas dessa violação sendo este um direito fundamental.

5 PENALIDADES IMPOSTAS

O objetivo deste capítulo é analisar as penas aplicadas aos crimes cibernéticos, como forma de coibir sua prática. Este é um dos objetivos mais complicados deste estudo, pois como mensurar um tempo de pena para tal crime que pudesse impedir ou ao menos coibir o seu cometimento?

Pois bem, analisemos o artigo citado abaixo:

“ [Art. 154-A.](#) Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”

Surge a dúvida se seriam estas penas de detenção de 3 (três) meses a 1(um) ano e de reclusão de 6 (seis) meses a 2 (dois) anos, apesar das suas majorantes, um meio de coibir a prática destes crimes.

Alguns agentes, no entanto, preferem correr o risco de serem condenados a estas penas em troca do risco de cometer o crime e tentar se esconder após o delito, pois terão um benefício satisfatório com o que conseguirem desta ação criminosa, caso não sejam encontrados.

No ano passado a Comissão de Constituição e Justiça e de Cidadania (CCJC) aprovou o Projeto de Lei 154/19 do Deputado José Nelto (PODE-GO), que altera o Código Penal afim de agravar as penas de crimes praticados no ciberespaço, deste modo o projeto segue aguardando análise pelo Plenário da Câmara dos Deputados.

Outro Projeto de Lei que segue para análise pela CCJC é o 4287/19, segundo a explicação da ementa:

Busca alterar os arts. 141 e 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar a disciplina dos crimes cibernéticos buscando acrescentar hipótese de agravamento da pena de crime contra a honra, quando cometido usando a internet, e tipifica a "Invasão de dispositivo informático", como a conduta de obter, adulterar ou destruir dados ou informações sem autorização do usuário do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Deste modo, o PL segue o mesmo intuito do anterior que já foi aprovado pela CCJC, agravando as penas dos crimes contra a honra quando cometidos usando a internet e tipificando a conduta de invasão de dispositivo informático. Buscando assim, mais severidade aos delitos cometidos no meio virtual.

6 CONSIDERAÇÕES FINAIS*

A evolução da sociedade acontece dia a pós dia, existem acontecimentos que revolucionam o mundo de um dia para outro e outros que vão sendo construídos e pensados devagar como forma de suprir uma necessidade, assim foi com o surgimento da internet, começou pela necessidade de comunicação entre grupos de guerra, na década de 60, durante a Guerra Fria. Desde essa época, até hoje, é imensurável o quanto este meio de comunicação se evoluiu.

O tema do presente estudo foram os crimes cometidos na plataforma virtual e a elaboração deste estudo surgiu da necessidade de verificar se as leis que vigoram sobre o tema, estão aptas a punir e coibir o seu cometimento.

Para tanto, abordamos o entendimento do funcionamento da plataforma virtual onde são cometidos tais delitos e posteriormente analisamos as normas vigentes que tipificam estas condutas, bem como as penalidades aplicadas a elas.

O presente estudo, expôs que o Direito busca evoluir para se amoldar aos casos de crimes que infelizmente ocorrem no campo virtual, assim como em vários outros campos, pois sempre estamos sujeitos a sermos vítimas de pessoas que buscam sempre se beneficiar de outras, nas mais diferentes e oportunas ocasiões.

Sendo assim, após este exaustivo estudo podemos considerar alguns pontos, como, sendo necessária a elaboração de novas leis para tipificar as condutas prevista neste tipo de crime, pois, estas não conseguem abranger tais condutas evolutivas, sendo que, as mudanças nos meios de execução dos crimes e as finalidades dos agentes tiveram grande evolução desde a criação das leis que vigoram em nossa legislação, sendo esta atualmente ineficiente. Quanto as lacunas evidenciadas neste estudo, apesar do Direito Penal não ter tipificação para tais ações, o ordenamento jurídico brasileiro se vale do direito a inviolabilidade da privacidade, conforme preceitua o artigo 5º, X da CF/88.

Outro ponto importante, constatado neste estudo é que um dos seus objetivos segue sendo atendido, qual seja o de aumento das penas cometidas nestes crimes virtuais devido a vulnerabilidade dos usuários, evidenciando assim, a importância do agravamento das penas praticadas nestes delitos, afim de coibir sua prática, se mostrando eficazes em sua aplicação em relação as punições aos agentes criminosos.

Outro lado é que, infelizmente também é possível constatar que ainda há uma enorme dificuldade com relação a encontrar o sujeito ativo destes crimes. E que o Estado deve investir mais na criação de meios eficazes para a identificação de seus usuários, para que, caso seja necessário, possa estar o “encontrando” e desta forma trazendo ao usuário de boa índole, maior segurança no acesso a

plataforma virtual que se faz tão útil e necessária nos dias atuais. Bom, o que se espera é que com o crescimento dos usuários e dos crimes praticados nesse meio, a legislação vigente consiga alcançar estes indivíduos que usam de meios ardilosos para se beneficiar e que consiga os punir, como forma de incentivar os demais usuários a não praticarem estes atos e não haver casos de reincidência por parte do sujeito ativo.

O Estado conta com a inteligência de seus servidores para encontrar meios capazes de suprir tais necessidades. Seria diante disso, possível a criação de um código por usuário? Como exemplo, os aparelhos, se cada um possui seu endereço IP, sendo capaz de o rastrear e encontrar, porque não cada usuário possuir o seu código, vinculado a seu CPF e digital, que possibilite acesso a todos os seus dados pessoais, podendo ser consultados mediante determinação judicial quando necessário. Obviamente, este meio também seria alvo de Crackers, que usariam destes códigos de acesso à internet para se eximirem de usar o seu pessoal. Pois bem, o Estado seria capaz de criar um meio de assegurar os cidadãos usuários da rede? Estaremos nos, seguros quanto a privacidade de nossos dados ao navegarmos nesta plataforma?

Uma coisa é certa, sempre estaremos vulneráveis, pois, apesar de existirem diversos meios de criar barreiras de proteção a nosso direito, intimidade e segurança, também existem meios de quebrá-los. Cabe ao direito tentar ao máximo reconstruir essa barreira que por hora pode ter sido destruída, buscando justiça a vítima, punição ao delinquente e reprimenda ao cometimento de tais crimes.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 28/06/2020.

BRASIL, Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília. Senado Federal, 2012. Acessado em 25 de junho de 2020.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

BRASIL, Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011.p.48

ESCOLA, Equipe Brasil. "Internet"; *Brasil Escola.* Disponível em: <https://brasilecola.uol.com.br/informatica/internet.htm>. Acesso em 01 de julho de 2020.

FERREIRA, Neto. Caminho até o servidor web. Disponível em: <https://netoferreira14.wordpress.com/2014/02/05/caminho-ate-o-servidor-web/>. Acessado em 30/06/2020.

FIGUEIREDO, Candido de. Novo Dicionário de Língua Portuguesa. 1913, p. 1122 e 2091 – Disponível em: <https://www.passeidireto.com/arquivo/19671152/dicionario-aurelio>. Acessado em 26 de julho de 2020;

GRECO, Rogério. **Código Penal Comentado,** Niterói: Editora Impetus, 2017.

HOESCHL, Hugo Cesar. *O ciberespaço e o direito.* **RTJE** – Revista trimestral de jurisprudência dos estados. São Paulo, ano 22, v. 167, nov/dez, 1998, p. 15-28.

NUCCI, Guilherme de Souza. Leis Penais e Processuais Penais Comentadas. São Paulo: RT, 2008.

OLHAR DIGITAL. Qual a diferença entre hacker e cracker. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024. Acessado em 30/06/2020.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

CONJUR. Violência virtual "Internet facilita crimes e dificulta investigação, estimulando a impunidade" Revista **Consultor Jurídico**, 5 de fevereiro de 2017, 7h39 - Disponível em: <https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais> . Acessado em 01/07/2020.

SANTOS, Raniere. Como a internet chega na sua casa. Disponível em <https://www.techtudo.com.br/noticias/noticia/2011/07/como-internet-chega-na-sua-casa.html>). Acessado em 26/06/2020.

SCHMIDT, Guilherme. **Crimes cibernéticos.** Jusbrasil, 2014. Disponível em: < <http://gshmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>>. Acesso em: 28 jun.2020.